ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Encrypting the Auto Detected Face Part of Human in a Image Using RC4 and Hiding the Data in Image

N.Mahesh Chandra
M.Tech Student,
Sreenidhi Institute of Science and Technology.

G.Sumalatha
Assistant Professor,
Department of Information Technology,
Sreenidhi Institute of Science and Technology.

Abstract:

In this paper, the concern of sending redundant data over a vulnerable, bandwidth-constrained connection channel. This paper discuss about sensitive image transferring over network. A content holder detects the face part of the human automatically in an image and the detected face part in the image is encrypted using RC4 algorithm. Perhaps, a data-hider considered bits of the encoded image utilizing a data-hiding key to generate a simple space to provide some extra information. Using data hidden key the recipient may acquire hidden data the recipient has no data around the initial sensitive image information. With help of the decryption key the recipient may acquire sensitive image data to get an image equivalent to the initial one, however can't acquire the hidden data. If the recipient has both data-hiding key as well as the encryption key, the recipient may acquire the further data also the initial image with no reduction.

Keywords:

Face part detection, Image encryption, image recovery, reversible data hiding.

1.INTRODUCTION:

As an efficient and prominent method for privacy safeguards, encryption transforms the standard signal into unintelligible information, to ensure the conventional signal handling normally occur ahead encryption or following decryption. Anyhow, in many situations that a content holder cannot trust the operating service vendor, the capability to control the protected data when preserving the basic information unrevealed is required. For example, when the hidden data to be sent are protected, a network provider with no information of the cryptographic key can usually shrink the protected data caused by the constrained channel source. resource is first condensed to its entropy level utilizing a ordinary source code. Therefore, the condensed source is protected applying among the many frequently obtainable encryption systems. At the recipient, decryption is carried out first, then decompression. Compression of protected data has enticed significant research desire [2]. The conventional means of safely and effectively sending redundant information is to initially compress the information to lessen the redundancy, thereafter to encrypt the condensed data to hide its significance.

At the recipient edge, the decryption as well as decompression functions are orderly executed to retrieve the initial data. Although, in many application situations, a sender requires to send certain data to a recipient and also intends to keep the data sensitive to a system operator in delivers the network resource for the relaying.However the sender must encrypt the initial data also the system supplier can usually compress the encoded data with no information of the cryptographic key as well as the initial data. At recipient edge, a decoder incorporating decompression as well as decryption features is utilized to restore the initial data.

TYPES OF ENCRYPTION:

a) Hashing Encryption
b) Symmetric Encryption
c) Asymmetric Encryption

SYMMETRIC ENCRYPTION:

This cryptography also known as private-key cryptography is among the earliest and many protected encryption techniques. The name "private key" occurs within the reality that the key utilized to encrypt as well as decrypt data should stay secure due to anybody with accessibility to it may understand the coded information. A sender encodes content into cipher text with a key; also the recipient utilizes the equivalent key to decode.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.FACE DETECTION ALGORITHM:

Voila-Jones Algorithm: The Viola-Jones algorithm uses Haar-like features, that is, a scalar product between the image and some Haar-like templates[6]. More precisely, let I and P denote an image and a pattern, both of the same size N _ N. The feature associated with pattern P of image I is defined by

$$\sum_{1\le i\le N}\sum_{1\le i\le N} I(i,j)1p(i,j)is\ white - \sum_{1\le i\le N}\sum_{1\le i\le N} I(i,j)1p(i,j)is\ black$$

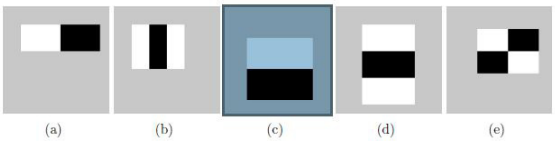

Figure 2-1: Haar-like patterns

Figure 2-1 shows five Haar-like patterns. The size and position of a pattern's support can vary provided its black and white rectangles have the same dimension, border each other and keep their relative positions. Thanks to this constraint, the number of features one can draw from an image is somewhat manageable: a 24 _ 24 image, for instance, has 43200, 27600, 43200, 27600 and 20736 features of category (a), (b), (c), (d) and (e) respectively, hence 162336 features in all.

Ada-Boost:

It helps Viola-Jones algorithm to select the best features and to train classifiers that use them. This algorithm constructs a "strong" classifier as a linear combination of weighted simple "weak" classifier.

$$f^T(x) = sign\left[\sum_{t=1}^{T} a_t\, h_t(x)\right]$$

Cascade Architecture:

Cascade of strong classifiers is arranged in a cascade in order of complexity, where each successive classifier is trained only on those selected samples which pass through the preceding classifiers. The job of each stage is to determine whether a given sub-window is definitely a face or may be a face. A given sub-window is definitely immediately discarded as not a face if it fails is any of the stages.

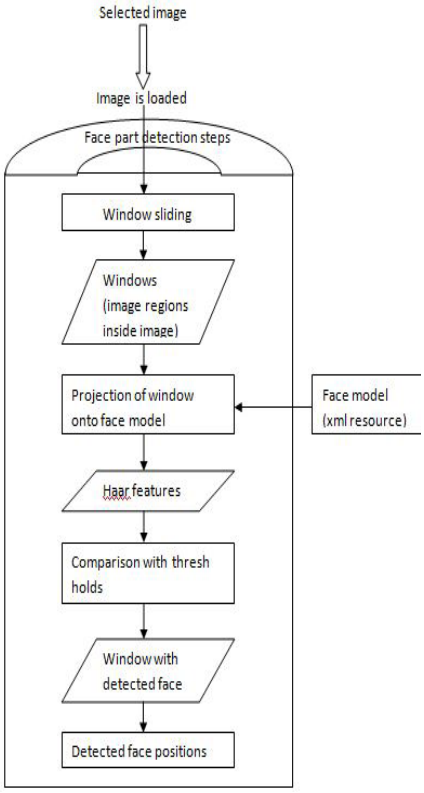

Figure 2- 2: flow chart of the face part detection

Figure 2-3: plain image

Figure 2-4: face part detected

3.DATA HIDING APPLICATIONSL:

•Covert connection utilizing images (secret content is concealed in a provider image)
•Tenure of digital images, verification, copyright
•Data consistency, fraud detecting, self-correcting images
•Including subtitles to images, extra details, like captions, to video, embedding subtitles or music tracks to video (video-in-video)

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

•Sensible browsers, regular copyright details, watching a film in a provided rated edition.
•Copy regulate (secondary shield for DVD)

4.NON-SEPARABLE REVERSIBLE DATA HIDING IN ENCRYPTED IMAGE:

A content holder encrypts the authentic image utilizing an encryption key; also a data-hider will embed increased data towards the encoded image utilizing a data-hiding key while the recipient cannot identify the authentic content. Because encrypted image incorporating excessive data, a recipient can initially decrypt it based on the encryption key, thereafter extract the integrated data as well as retrieve the authentic image based on the data-hiding key. In the strategy, the information extraction isn't separable from the information decryption. This means, the extra data should be taken through the decrypted image, to ensure the primary content of authentic image is presented before information extraction, also, if a person contains the data-hiding key yet not the encryption key, recipient can't extract every content from the encoded image that contains further data.

A. IMAGE ENCRYPTION:

Let an original image (plain-image) of n*m pixels. First, sender transforms the plain image into binary array. Let and be the plain image digit p(t), cipher image digit c(t) and key stream digit k(t) at time t. Then the encryption process can be described by the equation

$$c(t)= p(t) \oplus k(t)$$

B.GENERATION OF ENCRYPTION KEY :

Encoding key is 128 bit value. It is created arbitrarily with the arbitrary function. The arbitrary function creates the arbitrary key in a consistently delivered function. RC4 algorithm explained in Figure5-1.

C.GENERATION OF PSEUDO-RANDOM SEQUENCE:

Pseudo arbitrary sequence includes arbitrary bits created with the encryption key. In our strategy, RC-4 algorithm will be employed to generate the pseudo-random sequence utilizing the 128-bit encoding key. It is symbolized as series of bytes (An array of bytes) [3].

The amount of bytes created must be equivalent to the amount of pixels within the input image supplied the pixels are symbolized as 8-bit values. If the pixels tend to be symbolized as 16-bit values after that the amount of bytes in pseudo-random series must be double the amount of pixels.

5.RC4 ALGORITHM :

RC4 is a supply cipher, symmetric key algorithm. The same algorithm would be utilized for both encoding as well as decryption as the information stream is just XORed with the created key series. The key supply is absolutely separate from the plaintext utilized. It utilizes an adjustable length key from 1 to 256 bit to initialize a 256-bit specify table. The state table is utilized for consequent creation of pseudo-random bits thereafter to establish a pseudo-random stream that would be XORed using the plaintext to provide the cipher text. The algorithm is shattered into two phases: initialization, as well as operation. In the initialization phase the 256-bit state table, S is filled, utilizing the key, K as a seed. Whenever the state table is established, it remains altered in a frequent pattern as information is encoded. The initialization strategy is described by the pseudo-code. This algorithm generates a stream of pseudo-random standards. The feedback stream is XORed with such standards, bit by bit. The encryption as well as decryption procedure is just like the information stream is just XORed using the created key series. If it is provided in an encoded content, it can generate the decrypted content result, also if it is provided in plaintext content; it can generate the encrypted model [4]. The RC4 encoding algorithm is revealed in Figure 5-1.

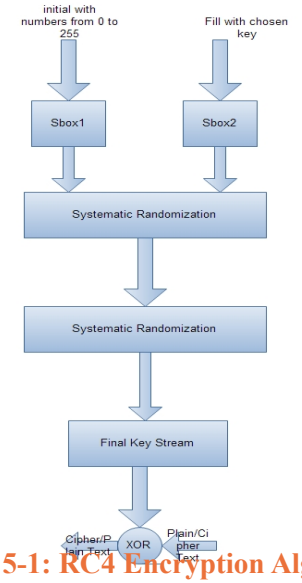

Figure 5-1: RC4 Encryption Algorithm

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A.RC4 Steps :

The steps for RC4 encryption algorithm is as observe:
1-Get the data to be encrypted and the selected key.
2-Create two string arrays.
3-Initiate one array with numbers from 0 to 255.
4-Fill the other array with the selected key.
5-Randomize the first array depending on the array of the key.
6-Randomize the first array within itself to generate the final key stream.
7-XOR the final key stream with the data to be encrypted to give cipher text.

RC4 algorithm features can be summarized

1-Symmetric stream cipher
2-Variable key length.
3-Very quick in software
4-Used for secured connections as in the encryption of traffic to and from secure websites using the SSL protocol.

6..RESULTS AND ANALYSIS:

To empirically evaluate the efficiency of our suggested technique, we've performed a number of tests. These tests incorporate: (i) encryption as well as decryption process, (ii) histogram analysis of plain-image and cipher-image, also (iii) key sensitivity analysis.

(i)Encryption and Decryption Process:

We utilize a 24-bit color image show in Figure 6-1. This image will be encoded with the secret key "abcdefghijklmnopq". The visual assessment reveals that the encoded image (cipher-image) location is absolutely hidden for human and also indicates that with the equivalent secret key, cipher-image might be transformed into plain-image as shown in Figure 6-2. This outcome reveals that our strategy performs effectively in both encryption as well as decryption process.

Security Analysis: In this segment, we reveal the security evaluation of the suggested image encoding algorithm like histogram analysis as well as key sensitivity evaluation regarding the plain-image as well as key to show that the suggested technique is resilient towards the analytical as well as brute force approach.

(ii)Histogram Analysis:

Preferably, the histogram of plain-image (Figure 6-1) as well as cipher-image (Figure 6-2) cannot provide statistical connection between one another. Using the histogram evaluation, we may observe that the histogram of every RGB channel is consistent. The consistent delivery of cipher-image histogram will be a pleasant indication where cipher is resilient towards statistical as well as brute force approach [5]. The outcomes of histogram evaluation usually reveal that there's no statistical connection around plain-image as well as cipher-image. Below figures are the plain image (Figure 6-1) and the ciphered image (Figure 6-2). Here we can see there is no statistical connection between plain and ciphered image.

Figure 6-1: plain image

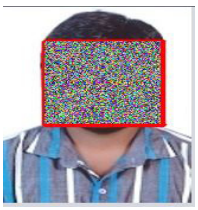

Figure 6-2: Face part is encrypted

(iii)Key Sensitivity Analysis:

We have performed a key sensitivity evaluation with a key which will be one digit varied from the original key to decrypt the encoded image. We come with encoded plain-image utilizing key "abcdefghijklmnopq" thereafter decrypted the cipher-image utilizing: (i) faulty key "abcdefghijklmnopr", also (ii) proper key "abcdefghijklmnopq". The ensuing image is completely assorted from the authentic image. This evaluation displays that the suggested algorithm is really vulnerable to any transform in the secret key value.

7.CONCLUSION: Pseudo arbitrary series contains arbitrary bits created with the encryption key. In our strategy, RC-4 algorithm can utilize to generate the pseudo-random series with the 128-bit encoding key.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The face part of the human in the image is detected and the detected part in the image is sending for the further encryption process. The face part pixels of the image are XORed with the key stream generated by the RC4 algorithm. The added data placed to encoded image with the variables. Through an encoded image incorporating extra data, the recipient can acquire the further info utilizing simply the data-hiding key, or acquire an image like the authentic one utilizing just the encryption key. Whenever utilizing both of the encoding as well as data-hiding keys, the enclosed further data may be effectively extracted as well as the authentic image may be absolutely restored by exploiting the spatial connection in normal image. Contrasted with another algorithm, the suggested strategy revealed effective consistency in retrieving the authentic images.

REFERENCES:

[1] X. Zhang, ―Lossy compression and iterative reconstruction for encrypted image,‖ IEEE Trans. Inform. Forensics Security, vol. 6, no. 1 pp. 53–58, Feb. 2011.

[2] W. Liu, W. Zeng, L. Dong, and Q. Yao, ―Efficient compression of encrypted grayscale images,‖ IEEE Trans. Image Process., vol. 19, no. 4 pp. 1097–1102, Apr. 2010.

[3] T. Bianchi, A. Piva, and M. Barni, ―Composite signal representation for fast and storage-efficient processing of encrypted signals,‖ IEEE Trans. Inform. Forensics Security, vol. 5, no. 1, pp. 180–187, Feb. 2010.

[4] William Stallings, Cryptography and network security: Principles and practice, Prentice Hall, Upper Saddle River, New Jersey, 2003.

[5] A. Jolfaei and A.R. Mirghadri, "An Image Encryption Approach Using Chaos and Stream Cipher," in Journal of Theoretical and Applied Information Technology, Volume 12 No 2, pp 117-125, 2010.

[6] Yi-Qing Wang "An Analysis of the Viola-Jones Face Detection Algorithm" Published in Image Processing On Line available online with the link at http://dx.doi.org/10.5201/ipol.2014.104.